ELSEVIER

Available online at www.sciencedirect.com
ScienceDirect
journal homepage: www.elsevier.com/locate/CLSR

Computer Law & Security Review

Backups and the right to be forgotten in the GDPR: An uneasy relationship

Eugenia Politou[a], *Alexandra Michota*[b], *Efthimios Alepis*[a], *Matthias Pocs*[c], *Constantinos Patsakis*[a,*]

[a] *Department of Informatics, University of Piraeus, Greece*
[b] *Department of Digital Systems, University of Piraeus, Greece*
[c] *Stelar Security Technology Law Research, Germany*

ARTICLE INFO

Article history:
Available online xxx

Keywords:
GDPR
Backup
Right to be Forgotten

ABSTRACT

The recent enforcement of the GDPR has put extra burdens to data controllers operating within the EU. Beyond other challenges, the exercise of the Right to be Forgotten by individuals who request erasure of their personal information has also become a thorny issue when applied to backups and archives. In this paper, we discuss the GDPR forgetting requirements in respect with their impact on the backup and archiving procedures stipulated by the modern security standards. We specifically examine the implications of erasure requests on current IT backup systems and we highlight a number of envisaged organizational, business and technical challenges pertained to the widely known backup standards, data retention policies, backup mediums, search services, and ERP systems.

1. Introduction

On the 25th of May 2018 the General Data Protection Regulation 2016/679 (GDPR) (Regulation (EU), 2016) has been put in force by the European Parliament and the Council of the European Union (EU) repealing the Data Protection Directive 95/46/EC (DPD) which for more than 20 years was setting out common rules for the data protection domestic legislation of the EU Member States. The GDPR intends, on the one hand, to strengthen and harmonize the well-established data protection legislation for all individuals within the EU, while on the other hand, to address the privacy harms emerged from the explosion of pervasive computing and the rapid change of data landscape in the big data era.

To confront these challenges the GDPR brings radical changes in the protection of the EU citizens' personal data and as a result impacts severely data controllers offering services within the EU. More precisely, the GDPR encompasses some new data protection principles for giving control back to individuals over their personal data such as the right to object to profiling, the right to data portability, and the obligation for data protection impact assessments. However, the most controversial and widely debated right anticipated by the regulation is the newly introduced Right to be Forgotten (RtbF) specified in the Article 17 of the GDPR.

The RtbF allows the retroactive erasure of one's personal data upon her request and from all available places they may have been disseminated. As we have already thoroughly discussed in Politou et al., 2018, the RtbF caused prolonged

[*] Correspondence to: Department of Informatics, University of Piraeus, 80, Karaoli & Dimitriou str., Piraeus 18534, Greece.
E-mail addresses: epolitou@unipi.gr (E. Politou), amichota@unipi.gr (A. Michota), talepis@unipi.gr (E. Alepis), mp@stelar.de (M. Pocs), kpatsak@unipi.gr (C. Patsakis).

https://doi.org/10.1016/j.clsr.2018.08.006

controversies due to its pivotal impact on current data processing procedures and its unavoidable conflicts with other rights such as the right to free speech and the freedom of information, especially in the era of big data and the Internet of Things (IoT). Of particular interest are the immense implications of the RtbF for the backup and archiving processes taking place within each organizational unit that handles personal data. Notably, already well-established backup and archiving procedures specified by state-of-the-art security models are affected significantly from the GDPR erasure requirements. In this regard, we analyze in this article the consequences of the RtbF implementation on the physical and cloud backup procedures along with its impact on the currently wide spread protocols and standards adopted in the design of most contemporary systems and frameworks.

The rest of this work is structured as follows. In the next section we discuss the GDPR in the context of the RtbF and its enforcement on the backups and archives. Afterwards, in Sections 3 and 4 we present and discuss the process of backing up along with the latest security standards that drive current backup and archiving procedures. In Section 5, the debate on enforcing the RtbF on modern IT systems is discussed and the envisaged issues arising from its implementation scenarios on organizational, business and technical level are analyzed. Section 6 concludes the article by discussing the way forward in terms of the theoretical and practical approaches for archiving in the GDPR era.

2. The GDPR and the right to be forgotten

The GDPR includes several legal data protection principles ranging from the traditional principles of data minimization, purpose limitation and lawfulness to the new principles of data protection by design and accountability (GDPR Articles 25(1) and 5(2), 24(1), respectively). Some other concepts also introduced by the GDPR are building on EU case law. For example, the RtbF in the GDPR extends the conventional data subject's right of erasure by requiring the controller to forward erasure requests to all recipients of personal data 0. Thereby, the RtbF as introduced by the GDPR constitutes an attempt of the EU to facilitate the erasure of obsolete personal data and thereby to respond to the challenges posed by the digital remembering. According to many scholars (Bannon, 2006; Blanchette and Johnson, 2002; Dodge and Kitchin, 2007; Mayer-Shönberger, 2011), the right evolves from the need for forgetting which is a central feature of our lives yet a topic having relatively little serious investigation by the social and computing sciences. The emergence of the RtbF in the GDPR diverges significantly from the right specified under the European Court of Justice for the Google Spain decision which actually regulated a "right to be delisted" since it aimed at the technological intermediary and not the original publisher of the information (Politou et al., 2018; Tirosh; Kulk and Borgesius, 2014; Bartolini and Siry, 2016). This way the GDPR adds to the data protection principle of data subject rights concerning transparency, access, correction and erasure, and data portability. Besides, the GDPR's reference to 'rights and freedoms' (as part of the risk-based approach, data protection by design, etc.) strengthens the role of the European Charter of Fundamental Rights (Charter of Fundamental Rights of The European Union).

In terms of the GDPR's enforcement on modern IT systems, some of its new principles and concepts are still under development. For instance, the principles of accountability and data protection by design (Pocs, 2012) are supported by self- and co-regulatory approaches in technical standardization. Whereas in the case of accountability, an international privacy management system is standardized and mapped to the GDPR (ISO/IEC 2nd CD 27552), in the case of data protection by design, a European approach is taken by means of a European Commission request for CEN, CENELEC and ETSI to develop a European Standard (EN) by 2019 (CEN-CLC/JTC 8/EN "Data protection and privacy by design and by default"), which might use international standardization such as concerning unlinkability and de-identification (ISO/IEC 27551, 20889) and consumer-centric standardization on privacy by design (ISO/PC 317/ISO 23485). Additionally, relevant sector-specific standardization is identified such as ISO/AWI 22697 "Health informatics – Application of privacy management to personal health information". Apart from technical standards, data protection authorities have adopted several opinions on the new principles of the GDPR such as the principle of privacy and data protection by design (European Data Protection Supervisor, 2018).

Concerning the relationship between the GDPR and technical solutions developed by research projects, the technological means analyzed in paper illustrate a way to support compliance with the GDPR. It should be noted that although technological means cannot ensure compliance with data protection obligations, can promote legal compliance. It is always the controller's (or processor's) responsibility to comply with those legal data protection obligations. However, it is not the technology as such that will comply with the GDPR requirements. In this case the research results serve as a tool to facilitate legal compliance.

For some law scholars, the RtbF enshrined in the GDPR does not actually represent a revolutionary change to the existing data protection regime because its roots lie within the right to erasure and the right to object, two well established rights under the DPD. For others, the right evolves from the national law in many European countries, such as France in which the Right to Oblivion is anticipated. Yet the GDPR brings some novelties in defining the right and the conditions under which it shall be invoked (de Andrade and Oblivion, 2014; Mantelero, 2013; Voss and Castets-Renard, 2016) inasmuch as foresees the condition of withdrawing consent (Article 17(1)(b)) in order the right to be triggered, a condition that has not been thus far encompassed in any national or European data protection law (Mantelero, 2013). Admittedly, this right comprises a breakthrough on the EU legislation domain as it does not only encompass the right to erase (or "to forget") but it also embraces the right "to be forgotten". While the first specifies the need for a controller to delete data, the latter implies the need for data to be deleted *from all possible sources* in which they reside. In other words, based on the GDPR, withdrawal of a previously given consent is one reason, among others, to have personal data erased by the controller not only from the one who processed the data in the first place but *from every data controller* who is processing the data (Article 17(2)). According to extended legal analysis (de Hert and Papakonstantinou, 2016; Bartolini and Siry, 2016), the right is a novelty and has a broader scope than any of the existing rights whereas its unique feature that makes it different from the rights granted by the existing legislation is its retro-activity.

Nevertheless, the article 17(3) of the GDPR allows for some exemptions from the “forgetting” requirement, e.g. for cases of *compliance with a legal obligation or in the exercise of controller’s official authority* 17(3)(b), and *for archiving purposes in the public interest, scientific or historical research purposes* 17(3)(d). Clearly, the exemptions described by the 17(3)(d) may as well refer, for many controllers, to the instances of their archived data. However, article 89, which provides “*derogations relating to processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes*”, does not include the RtbF (Article 17) as a potential exemption. What perplexes more the issue is the mismatch between Article 89 and Recital 156 as the later does provide for a derogation from the Article 17 when personal data are processed for the same purposes.[1] And although the recitals are not legally binding texts, yet the conditions under which an exemption from the RtbF is allowed are not crystal clear. Furthermore, as the Article 17(3)(b) clearly mandates, for certain cases other legal obligations stipulating data retention by the controllers will prevail over the GDPR’s provisions.

From the above, it is evident that the enforcement of this right would pose major technical challenges due to the practicalities involved in knowing all the controllers who are processing the personal data in question. Even when controllers do have knowledge of the third parties processing some data that they collected, it places upon them the additional obligation to inform those third parties about the erasure request (Article 17(2)). Whereas the GDPR provides a convenient exemption from the obligation to inform all recipients of any rectification or erasure when this *“proves impossible or involves a disproportionate effort”* (Article 19), this exemption has also raised some concerns regarding the effectiveness of the RtbF as its scope of applicability is not always obvious (European Data Protection Supervisor). In the final analysis, controllers are required to implement technical solutions not only to allow the tracking of personal information but also to prove its efficient removal in the case of request for erasure under the GDPR. And although the first may not be considered a difficult task, since many controllers keep links of their copied information, the burden to prove that the erasure has been implemented successfully from all available sources is still technologically questionable. Taking further into account that the personal data may have been already backed up or archived by the controller or by the third parties, and then the practical difficulty for implementing this requirement seems indisputable. As a matter of fact, implementing the RtbF requirement for personal data that have already been backed up or archived is deemed to be not an easy task.

Before proceeding with the feasibility study of enforcing the GDPR in real case backup scenarios, we will describe below what a backup process entails and the most prevailing international security standards specifying backup procedures.

3. The process of backing up

In general, backup is “*a copy of information held on a computer that is stored separately from the computer*”.[2] Backups are considered to be fundamental processes within the business continuity plan as they allow for recovery when an information system suffers a disaster. The disaster may stem from various sources that include malicious actions, e.g. cyber attacks, but also physical damages, hardware failures and system crashes. Therefore, backups goal is not data preservation, but quick recovery. Eventually, backup is a repeated process whose regularity depends on the criticality of the system and the data it stores. Considering the enterprises, it has already been shown that the data loss phenomenon leads to serious financial loss in the scale of billions per year (Kovacs, 2014).

Practically, a backup is a copy of organization’s data in a specific timeframe that can be recovered in case of a disaster. In fact, according to the dictionary of Storage Networking Industry Association (SNIA),[3] the Point In Time copy (PIT copy) is “*A fully usable copy of a defined collection of data that contains an image of the data as it appeared at a single instant in time. …Implementations may restrict point in time copies to be read-only or may permit subsequent writes to the copy*”. Therefore, each backup is stored in specific data formats, on specific mediums and is marked based on the employed system/software and the timestamp to trace the time instance it reflects. To guarantee its availability, the storage media undergo scheduled checks and to verify its integrity, each backup is digitally signed, and a log of these records is securely stored.

Although archives are often inseparably associated with the notion of backups, still they distinguish from each other in many aspects. While backups are primarily used for fast operational recoveries by taking periodic images of active data, which are retained only for a few days or weeks, archives are typically designed to provide ongoing rapid access to years of business information by storing versions of data that are no longer in use, not changing frequently and not required on a regular basis.

There are various types of backups that can be categorized by their content, their medium or their method. For instance, based on the content we can have simple copies of some files, database dumps, full system images and snapshots. The choice of its content is normally subject to the restrictions an organization has on recovering for a specific system. Therefore, for highly critical systems that need to be instantly recovered, a snapshot of the system is stored and loaded when deemed necessary. The latter applies to cloud instances and to virtualized systems in general. Backups also vary in terms of the medium, as they may be stored in different

[1] *“Member States should be authorized to provide, under specific conditions and subject to appropriate safeguards for data subjects, specifications and derogations with regard to the information requirements and rights to rectification, to erasure, to be forgotten…”.*

[2] https://dictionary.cambridge.org/dictionary/english/backup.

[3] http://www.snia.org/sites/default/files/SNIADictionaryV2015-1_0.pdf.

mediums due to cost and durability constraints. Moreover, to reduce space requirements, we have incremental backups, which contain only the data that have changed since the preceding backup, and differential backups, which contain only the data that have changed since the previous full backup.

A well-known strategy for backups is the 3-2-1 rule. The core idea of this strategy is to minimize possible failures during the process of storing and recovering a backup. According to this rule, one must keep at least three backups. These three backups must be stored in two deferent mediums. From these three backups, one backup must be off-site.

4. The standards

In this section we present the most widely adopted international standards for IT security assurance, and especially those concerning backup procedures. Generally speaking, standards set the primary requirements that lead to regulatory compliance and they are commonly categorized by region and/or by sector. For instance, the Health Insurance Portability and Accountability Act (HIPAA) (Health Information Privacy, 2015) is a US regulation framework for ensuring the confidentiality and security of Protected Health Information (PHI) while the Payment Card Industry Data Security Standards (PCI-DSS) (PCI Security Standards Council) is a financial industry standard aiming to protect payment card data used in transactions.

In the IT security domain, several standardization bodies, such as the International Organization for Standardization (ISP), 2011, the American National Standards Institute (ANSI) (American National Standards Institute), the Canadian Standards Association, 1995, and the Standards Australia, have developed security and privacy frameworks that may be incorporated in organizations' processes and procedures to protect their data assets. These standards recommend also methodologies for IT governance, risk identification, security controls, and information security. More specifically, the ISO/IEC 38500 (ISO 38500, 2015) introduces an IT governance framework that provides guidance in the case of cloud services. ISACA organization created a methodology named COBIT (Control Objectives for Information and Related Technology) for better information management and IT governance. The National Institute of Standards and Technology (NIST) Cybersecurity Framework (CSF) is a policy framework that focuses on the security of US businesses and private organizations against cyber attacks. Last but not least, the ISO/IEC 27000 series of standards (I. I. O. for Standardization, 2011) is probably the most widely known and used set of standards relating to the security of Information and Communication Technology (ICT) systems. In particular, ISO/IEC 27001:2013 (ISO – International Organization for Standardization, 2013a) provides guidelines for mitigating risks of data breaches and fully supports the requirements of an information security management system while ISO/IEC 27002 (ISO – International Organization for Standardization, 2013b) provides best practice recommendations on information security controls. The ISO/IEC 27017 (ISO – International Organization for Standardization, 2015a) is based on ISO/IEC 27002 and gives guidelines applicable to the provision and use of cloud services.

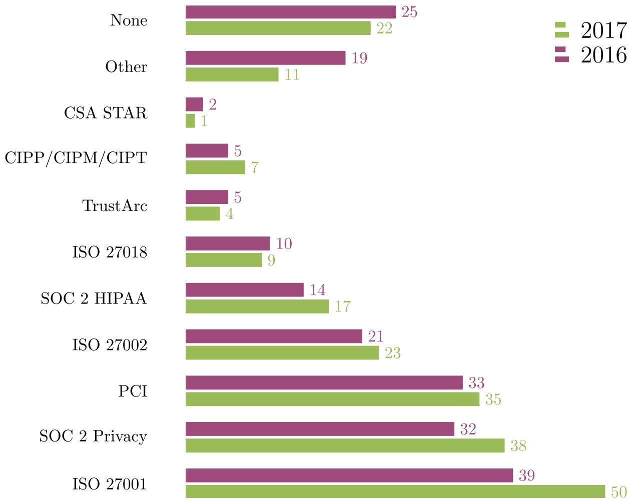

Fig. 1 – Third party audits/certifications required from vendors. Source: IAPP-EY Annual Privacy Governance Report 2017 (IAPP-EY, 2018).

The compliance of an organization with the specifications of a standard is formally accomplished and demonstrated through specialized audits and respective certifications. As seen in Fig. 1, third party audits and certifications are most of the times set as prerequisites by vendors to ensure that the auditee is in compliance with regulatory mandates. Third party audits are conducted by independent bodies to verify that an organization conforms to the requirements of a chosen standard and continues to meet these requirements on an ongoing basis.

Backup compliance requirements are not referring just to the storage process of the data lifecycle. Instead, they cover a set of procedures that should be followed for keeping data assets securely and efficiently and, along with the backup restoration requirements, participate substantially in the Disaster Recovery and Business Continuity plans. The appropriate policies for backing up personal data require an initial data mapping to be performed that should be then followed by an effective data governance model specifying how these personal data are to be managed in backups. In particular, the type of data that needs to be protected as well as the associated risks and privacy impact in case of a data breach must be clearly defined. On top, the methods and the means the data are stored and backed up as well as the relevant locations, including any off-site and on-site storage options, and the access to them should be specified. After mapping the data and establishing the appropriate data governance model, assurance that backups are well protected, and in special cases encrypted, should be provided. Furthermore, suitable measures ensuring that backups are kept only for a specified time need to be taken.

Likewise to security, backup policies and procedures are subject to the various requirements stemmed from the legal and regulatory frameworks. Although backup compliance is difficult to be achieved due to the growing number of both legal and regulatory requirements, the appropriate frameworks and standards selected for backup and recovery compliance navigate pertinently through the requirements need to be met.

Given the importance of data in every organization's operations, backup procedures are addressed by almost all security standards and frameworks, including COBIT, NIST (Joint Task and Initiative, 2013) and Cloud Security Alliance (CSA) Cloud Controls Matrix (CCM) (Cloud Security Alliance). Under the ISO/IEC 27000 series (I. I. O. for Standardization, 2011) the backup procedures are covered by the ISO 27001:2013, (12 operations security, 12.3 Backups) in conjunction with the ISO 27040:2015 (ISO – International Organization for Standardization, 2015b), which provides security and data protection guidance for storage systems. Additionally, the ISO/IEC 27018 standard (ISO – International Organization for Standardization, 2014), which is based on both ISO/IEC 27001 and ISO/IEC 27002 standards, provides additional guidance for the personally identifiable information (PII) stored and processed in public clouds and addresses storage and backup procedures taking into account the privacy principles of the ISO/IEC 29100 standard – Privacy Framework (International Organization for Standardization, 2011). Relevant also to the backup processes is the NIST Special Publication (SP) 800-88 which, in conjunction with NIST SP 800-53, provides guidelines on sanitizing data storage media. Furthermore, in the case of terminating a cloud service used for maintaining backups, a well-defined and documented exit process is described in the CSCC document Practical Guide to Cloud Service Agreements (Cloud Standards Customer Council (CSCC), 2015).

5. Problem setting

As already mentioned, a major issue arising from the obligation for erasure requests under the GDPR RtbF concerns the case where personal data have already been backed up or archived. The issue is increasingly occupying the IT industry since any noncompliance may cause high sanctions. To this respect, technical experts are debating on whether the RtbF should apply to the backups in the first place.[4,5] Taken into account the enormous cost and effort of implementing the RtbF into the real-world backup and archive data stores, they argue that the most convenient interpretation for the RtbF to backups or archives would be not to be applicable at all. Yet this view is not followed by most legal experts due to the absence from the GDPR text of any definite relevant exemption. As a matter of fact, the regulation does not provide any clear and unambiguous definition of the RtbF regarding its non-trivial practicalities of enforcing such a deletion when secondary uses apply, i.e. personal data have been disseminated to third parties, they have been anonymized or pseudoanonymized, or they have been backed up and archived.

As both sides have valid arguments, the issue of how the RtbF is to be implemented on real IT systems is expected to be clarified upon an explanatory interpretation by an official EU data protection body such as the EDPS. Nevertheless, as up to now there is neither a clear basis nor an explicit derogation for backups within the GDPR text, it is reasonable to argue that the RtbF is indeed applied to backups as well. In fact, the UK ICO, while has already provided guidance arguing that deletion should also apply to the backups,[6] recognizes in the meantime that deleting information from a system is not always a straightforward matter and hence sometimes it is preferable to put information "beyond use" providing appropriate safeguards for these cases.[7]

Notwithstanding this debate, the majority of the IT community agrees that the impact of the RtbF on the short-term backups, which are normally retained for a limited period of time to ensure business prompt recovery from accidental destroy or corruption, will be minimal comparing to the long-term archival backups that represent the long-term storage of the organization's history records and they are used for future reference. Acknowledging this disproportionality, and for the sake of clarity, we clarify that when the term backup is used hereafter it refers to the case of the long-term archival backup.

To overcome the oxymoron of having data deleted from archives while they have taken in the first place to safeguard the exact image of the data at a specific point in time, several solutions have been proposed. These include cryptographic erasures in which every record in a database is encrypted upfront with a different encryption key and upon a removal request the relevant encryption keys are deleted.[8] As a matter of fact, this method actually deactivates the personal data in question, rather than removing them.

A second solution proposed by several analysts is to keep a separate table of all forgotten user IDs from the "live" system and each time a backup is restored, the forgotten users are checked against its contents and they are being re-forgotten.[8] Although this method seems a convenient workaround as it does not deal at all with the backups, it is questionable if it is appropriate to fulfill the GDPR requirements given the fact that the IDs in the separate table still constitute personal data, since with the use of additional information they can single out a specific person, and hence the problem of forgetting them from backups remains. What's more, it does not deal with the case where a person requires to remove only specific pieces of her personal information instead of all of it or when a portion of her information needs to be retained according to other legal requirements. Furthermore, none of the proposed approaches deals with the onerous matter of unstructured personal data, such as emails or files, when they are needed to be removed from backups.

[4] https://www.linkedin.com/pulse/gdpr-right-forgotten-backups-jan-garefelt/.

[5] http://www.gdprarticles.com/gdpr-articles/data-subject-rights/gdpr-right-to-beforgotten-include-backups/.

[6] https://ico.org.uk/for-organisations/guide-to-data-protection/principle-5-retention/.

[7] https://ico.org.uk/media/for-organisations/documents/1475/deletingpersonaldata.pdf [8]https://axoniq.io/events/2017/11/gdpr-webinar.html.

[8] https://techblog.bozho.net/gdpr-practical-guide-developers/.

Utterly, the implementation of the RtbF in the digital environment is not a straightforward task while its effective enforcement in the backups may be proved burdensome or even impossible in a number of scenarios. To emphasize the potential issues we identify and analyze below some affected areas on the organizational, business and technical domain.

5.1. *Implications for the standards*

The RtbF that individuals may exercise under the GDPR involves requests of erasure of all or part of their personal data. As mentioned earlier, when these requests are received by a data controller the relevant data have to be removed under a specific timeframe from all the sites they reside, including archives and backups. Although the GDPR allows for exemptions from the RtbF when other legal obligations enforce the retention of these data, it is expected that the well-established international standards driving and specifying backup procedures will most likely be questioned and challenged under the new law.

This is due to the fact that the basic concept of backup specified by these frameworks and standards mandate the storing of exact copies of the data as a fall-back mechanism that organizations should use only when things "go wrong", e.g. there is a physical medium failure, a disaster or a cyber attack. Hence the standards consider the backups to be immutable and thereby they are specifying that, apart from disruptions, the backup media should be tampered with only to check their health status.

Examples of standards that would be affected from the GDPR erasure requests are spread throughout the domains. In the US, HIPAA CFR 164.308 (7) (ii) (A) mandates:

> *Data backup plan (Required). Establish and implement procedures to create and maintain retrievable exact copies of electronic protected health information*

This may impact severely products and services compliant with HIPAA standards such as the Service Organization Control (SOC) 2 HIPAA.

According to the ISO/IEC 27001 and 27002 Section 12.3.1, which specify that:

> *Adequate backup facilities should be provided to ensure that all essential information and software can be recovered following a disaster or media failure.*

one may rationally deduce that the backups cannot or should not be edited, as each data modification would not only affect the data but also the entire backup which by definition represents a unique instance at a given timestamp. The above concerns are also applied to ISO 27018 which adopts the backup procedure of 27002 with minor sector-specific guidance. Similarly, ISO 27040, Section 7.4.1., states that "*archival storage assumes a write-once, read-maybe access pattern, thus the integrity of the data in the system should be actively checked at regular intervals rather than waiting to when it is read*", indicating the immutability property of the archived information which is only read but not overwritten nor deleted.

In the case of PCI-DSS, Section 10.5 of version 3.2[9] requirements reads as follows:

> *10.5 Secure audit trails so they cannot be altered.*
>
> *10.5.1 Limit viewing of audit trails to those with a job-related need.*
>
> *10.5.2 Protect audit trail files from unauthorized modifications.*
>
> *10.5.3 Promptly back up audit trail files to a centralized log server or media that is difficult to alter.*
>
> *10.5.4 Write logs for external-facing technologies onto a secure, centralized, internal log server or media device.*
>
> *10.5.5 Use file-integrity monitoring or change-detection software on logs to ensure that existing log data cannot be changed without generating alerts (although new data being added should not cause an alert).*

Moreover, the standard mandates in 10.7 to:

> *Retain audit trail history for at least one year, with a minimum of three months immediately available for analysis (for example, online, archived, or restorable from backup).*

While the standard in the above sections focus more on attacks from outsiders, it mandates that audit trails must not be altered and, regardless of other changes, the data must remain, even in the backups, for at least a year.

Plausibly, all the above standards, which according to Fig. 1 are among the most required standards in the market, present serious inconsistencies with the GDPR RtbF requirement and may result in difficult situations when organizations have to strike a balance between the new regulation and the already widely spread well-known standards and best practices. While the compliance of the GDPR erasure obligations with the backup requirements mandated by the state-of-the-art security standards such as the ISO27000 series occupied recently the interest of both the research (Bartolini et al., 2015) and the security community,[10],[11],[12] hitherto there has not been any comprehensive studies on this subject. Therefore, we argue that an immediate alignment of the standards with the GDPR provisions, and specifically with the RtbF, is deemed necessary and urgent. Otherwise, organizations, due to their high dependency on certifications and standards, may be severely affected.

5.2. *Implications for the data retention policies*

While the GDPR does not mandate a specific timeframe for which personal data must be kept, data have actually a specific lifespan. In fact, data retention periods are determined by sector-specific business requirements and relevant domestic legislations. The storage limitation principle, according

[9] https://www.pcisecuritystandards.org/documents/PCI_DSS_v3-2.pdf.

[10] http://www.iso27001security.com/ISO27kGDPR-mapping-release1.pdf.

[11] http://www.iascertification.com/free-iso-27001-Checklist.pdf.

[12] https://advisera.com/wp-content/uploads/sites/15/2018/03/List_of_documents_EU_GDPR_ISO_27001_Integrated_Documentation_Toolkit_EN.pdf.

to which "*personal data shall be kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed*", has been enshrined in the EU data protection law since the DPD era. Of course, there are exceptions insofar as the personal data are processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes (GDPR-Article 5(1)(e), DPD-Article 6(1)(e)). As a result, it can be safely reasoned that all contemporary systems that are processing, and thereby archiving, personal information are aligned with sector and domain specific retention requirements ensuring that data in the backups are not kept for more than it is necessary.

Yet the GDPR obliges the data controllers to ensure that the period for which the personal data are stored is limited to a strict minimum (Recital 39) and also to maintain a record, where possible, of their processing activities which shall include, among others, the envisaged time limits for erasure of the different categories of data (Article 30(1)(f)). Furthermore, the GDPR introduces stricter rules for facilitating the transparency of the process when data subjects are exercising their rights. To this end, it removes any fees relating to the administrative costs when controllers are being requested to remove any personal data under the RtbF, unless the request is *manifestly unfounded or excessive* (Article 12(5)), and specifies stricter timescales for responding to user requests for data erasure. More precisely, the GDPR enforces controllers to proceed with the erasure request *without undue delay and in any event within one month of receipt of the request* (Article 12(3)). This period *may be extended by two further months where necessary, taking into account the complexity and the number of the requests*.

Apparently, these new requirements may present some technical challenges mainly due to the fact that user data are not stored within a single system, but they are spread across multiple applications and storages, off-site and onsite, and they may be found under various forms such as emails, files, database records etc. Worse still, these data may have been already archived. To complicate even further, user data may have been archived in multiple backup files originated from various applications where they are used in. On top, they may have been included in many copies of the same backup file since backups for the same data are taken in regular periods of time. Last, typically each backup file includes data from many users. All the above imply that controllers need to search, identify and remove, in an efficient and timely manner within both the production and backup environments, any relevant personal data an individual requested to be erased.

By exploiting economies of scale, many companies outsource their storage management, avoiding thus the costs of maintaining a data center. This shift has also been applied to backups as both cloud storage and backups are based on the same concept and are performed more or less by the same service providers. In terms of the security, the general concerns about cloud backups are more or less the same as with the cloud storage. In this regard, cloud backups must ensure proper encryption of the data, at least during transfer, while simultaneously it is essential to know where the backups are located in terms of geographic area as this, due to the diversity of data protection legislation across countries and continents, may entail issues with jurisdiction and fair information practices. Nevertheless, in the cases of cloud services, the providers do not know where the data of individual users reside, as by definition a cloud provider is agnostic of the data that stores.

Consequently, and regardless of whether the backups are performed on the cloud or not, it is of utter importance the data controller to keep track of the contents of each backup so that to either erase later by himself or to request from the service provider to remove any requested information. It should be noted also that for the personal data to be entirely removed they should not be simply deleted from the backups, but they have to be wiped.

5.3. *Implications for the mediums*

Irrespective of the followed security standards, the common practice for backup procedures are to oblige organizations to keep backups in the form of disks, which may vary from optical CDs, DVDs to even blueray discs and hard discs, or in tapes. While the cost per gigabyte for large capacity disk drives is constantly decreasing, tape backups are still cheaper. Regardless of whether full or incremental backups are performed by an organization, it follows that when data are needed to be removed from one copy, all the subsequent copies must be altered accordingly.

While the digital records used and stored within the production systems can be easily removed once they are located, the same does not apply for the already backed up or archived data for which big effort, and hence further cost, is required. For instance, in the case of optical discs the data cannot be erased at all. As a result, when a user requests removal of her data new copies of all the subsequent backup discs, since user's first data storage, have to be made with the requested data omitted and the corresponding discs destroyed. Even in the cases of hard discs and tapes where there is no need to destroy the actual storage medium, not only the relevant data have to be deleted but additionally all the following backups need to be appropriately altered.

Tampering with the backups is by no means a straightforward procedure as the stored data might be in a deprecated format, a fact that requires additional effort for efficiently searching through its contents, while the resulting new backups need to be properly signed and filed to ensure accountability in case of errors or undesired changes.

It should be highlighted that while for some export formats deleting single records from the backup are typically allowed without needing to restore the full database, for tape backups this is impossible as tapes store data in sequential blocks and therefore cannot be randomly accessed. Therefore, deleting a record from a database table that resides in a tape backup implies the restoration of the whole database, thus increased cost and complexity.

5.4. *Implications for the search services*

Even when deleting single records from backups is typically allowed in order to conform with the exercise of the RtbF by individuals, searching into vast backup archives for particular personal data is by no means an easy task. In reality, searching into backups for particular files is not a relative new feature

Please cite this article as: Eugenia Politou et al., Backups and the right to be forgotten in the GDPR: An uneasy relationship, Computer Law & Security Review: The International Journal of Technology Law and Practice (2018), https://doi.org/10.1016/j.clsr.2018.08.006

patented (Nene et al., 2011; Tsaur et al., 2015; Lyons et al., 2016) and several business tools,[13,14,15] are already offering similar services. Recently, more sophisticated backup indexing and searching tools have emerged, such as the one provided by the Dell EMC Data Protection (DP) Search[16] which introduces unified index, search, and recovery features allowing easily backup search via a Google-like keyword search.[17] Nevertheless, none of these tools are scalable enough, especially when they need to search almost rapidly into massive archived storages of mostly unstructured data, which is still the most common type of data in every organization.[18,19]

Apparently, current technology seems to fall behind in methods for efficient search algorithms capable to look across the entire data landscape in a cross-platform and a cross-format manner without any noticeable delays. As a result, for effectively implementing GDPR-compliant backup and archiving search services, the technological limits of data processing are clearly required to be expanded.

5.5. *Implications for ERPs and analytics*

Over the last decades, organizations worldwide have adopted ERP (Enterprise Resource Planning) software in order to automate and manage their business processes. Some of the most common ERP systems incorporate modules for product planning, purchases, supply chain, procurement, inventory control, product distribution, human resources, accounting, marketing and finance. Integrating these modules into a single system is considered as a prerequisite for an ERP system whose actual potential lies in using the data for analytics, data driven business decisions, risk reduction, fast-track reporting and performance management.

Initially, ERP systems targeted more on the back-office software leaving the front-office functions to be dealt with cooperating software such as CRM (Customer Relationship Management) systems that communicated with customers in a more “direct” way. Nevertheless, modern ERP solutions integrate front office components, including even software solutions for mobile devices. Moreover, present-day ERPs also provide enterprises with functionalities to collaborate with their peers, realizing system-to-system interaction and data exchange.

Within a business workflow there is a variety of data streams that include personal or sensitive user information which is subsequently backed up. These data streams originate from fundamental software modules, such as the Business Intelligence (BI) module, the Customer Relationship Management (CRM) module, the Front-Desk module, email interfaces and, as illustrated in Fig. 2, other modalities of user interaction, such as mobile phones and web pages.

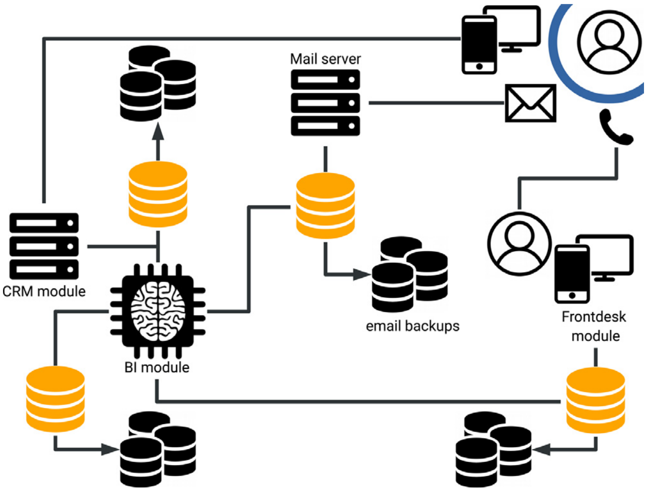

Fig. 2 – Backup data collected from different streams within business workflows.

Apparently, a software solution that collects, stores and analyzes data of personal nature, e.g. related to customers, needs to oblige to data protection laws and hence to the GDPR RtbF provision. By examining primarily the storage and consequently the backups of the involved personal data, perhaps the two most profound questions are whether it is possible to locate and erase personal data, when required, in a specified timeframe and whether these operations will hold back or even disable some of the ERPs’ back-end functionality.

Locating the Social Security numbers or other key personal data in tens or even hundreds of thousands of distributed tables of e.g. a SAP ERP system (one of the most widely used ERPs to date) is not trivial[20] as this information is not always directly linked with the user ID of one database. Personal data discovery on systems of such magnitude and complexity could require enormous amount of time and effort. Taken also into consideration that the GDPR, as we mentioned earlier, enforces specific and strict time constraints for controllers to respond to a user request for either deleting or accessing her personal data, the tasks of locating and removing specific piece of personal information from ERPs may face several challenges in the days to come. These challenges can be further intensified due to the fact that the backup plans of ERP installations may significantly vary in terms of the means used (e.g. cloud infrastructures, hard copies) and the actual backup operations which range from daily database tables’ copies to full ERP system image backups.

[13] https://support.code42.com/Administrator/5/Monitoring_and_managing/File_search/01_Enable_file_search_in_your_Code42_environment.

[14] https://docs.druva.com/001_inSync_Cloud/Cloud/030_Governance_DLP/030_Governance_and_DLP/010_Governance/020_Enterprise_Search_for_backed_up_data.

[15] https://helpcenter.veeam.com/docs/backup/em/searching_vm_backups.html?ver=95.

[16] https://uk.emc.com/collateral/TechnicalDocument/docu58859.pdf.

[17] https://blog.dellemc.com/en-us/make-it-rain-with-your-emc-hybrid-cloud/.

[18] https://breakthroughanalysis.com/2008/08/01/unstructured-data-and-the-80-percent-rule/.

[19] https://www.emc.com/about/news/press/2012/20121211-01.htm.

[20] https://www.silwoodtechnology.com/blog/tested-5-erp-and-crm-packagesevaluated-for-gdpr-personal-data/.

State-of-the-art ERPs already provide their enterprise customers with tools that can facilitate GDPR compliance in specific domains. For instance, SAP offers five tools to help address GDPR needs, namely the SAP Information Lifecycle Management, the SAP Data Services, the SAP Information Steward, the SAP Process Control, and the SAP Access Control. Yet there are more tools for GDPR compliance available which can be categorized according to their key functionalities as follows:

- Tools that enable ERPs to discover where personal data are located in their systems.[21],[22],[23],[24] While these tools can locate personal data residing in current systems, it is not clear whether they are able to locate personal data that have already been backed up. In order to achieve this, these tools should incorporate special logging mechanisms keeping track of backup data in their real-time databases.
- Tools that enable the deletion of personal data.[25] Since locating data does not necessarily mean deleting them, these functions are being investigated completely separately. This kind of tools is necessary to enable the "safe" deletion of personal data both for security and stability reasons since, apart from a secure data removal, there is a need for a guaranteed "stability" of the ERPs following the required deletion operations. As these tools can affect the integrity of the data, plausible challenges include the safekeeping of system's integrity when the removal of data both from backup and production environments is requested, as well as the successfully erasure of data that have been communicated with other parties (and possibly also backed up).
- Tools for managing and auditing the access to the stored personal data. These tools provide rules for reading and changing data files and hence they are essential towards the application of the new regulations.[26] Nevertheless, these tools refer to the run-time instances of the data and therefore it is not clear how these rules for managing access to personal data are going to be applied to the backup versions of the data.
- Tools for masking personal data. As already mentioned, ERP systems are able to integrate a large number of complex functions that include analytics, reporting and business decisions. Therefore, the elimination of a smaller or bigger part of a past database may affect the data analytics already produced or are to be produced in the future. To this end, an alternative to data deletion could be considered the masking of personal data. If this is deemed as the desired option for a use case, given the fact that the GDPR foresees for cases where the removal of personal data is indeed impossible *taking into account the available technology and the cost of implementation*, then the masking of all corresponding backed up personal data must also be ensured. However, many tools for masking personal data do not apply such changes to the production systems, let alone backups,[27] as the results may break the integrity of the system.

Table 1 – Archived objects from a retail sale.

New user	User transaction
Name	Date of transaction
Surname	Time of transaction
Billing address	User who performed the transaction
Shipping address	The place the transaction took place
TIN/TRN	The method of payment
Method of payment	The payment terms (e.g. installments, cash on delivery)
Bank information	The billing address and shipping address of that particular transaction
	The payment card number (encrypted) with which the payment may has been made
	Items bought in the transaction
	Quantity bought
	Price
	Discounts

5.6. *Archived ERP data use cases*

To thoroughly study the extent that the GDPR regulation, and in particular the RtbF, affects the already established business operations, including backups, we illustrate below a number of use cases evolving from real case ERPs scenarios. More specifically, in what follows we present the sets of data fields that are stored and consequently backed up for a given customer under a well-known ERP installation for the telecommunications industry.

When a retail sale is performed, with invoice included, the ERP first checks if the corresponding customer exists in the system via a unique key field (e.g. Tax Identification/Registration Number-TIN/TRN). Following each user transaction, personal data relevant to the specific transaction are saved. An indicative list of personal data stored in such cases is illustrated in Table 1.

During dunning a significant set of personal data are collected, stored and archived. Dunning involves the process where a company communicates with its customers in order to insure the payment of their due amounts, a very common process supported by the ERP functionality. The communication is usually achieved with SMS messages, calls from representatives, and emails. The data objects that can be archived from the dunning process include:

- Phone calls made to the customer.
- SMS messages sent to the customer.
- Legal offices the customer was assigned to.

[21] https://www.7safe.com/digital-investigation-services/ediscovery/IPDAR.
[22] https://www.silwoodtechnology.com/safyr/safyr-7-supporting-gdpr/.
[23] http://filefacets.com/product/.
[24] https://www.netmail.com/data-federation-software.
[25] https://www.trustarc.com/products/individual-rights-manager/.
[26] https://www.trustarc.com/products/individual-rights-manager/.
[27] https://www.epiuselabs.com/data-secure.

Please cite this article as: Eugenia Politou et al., Backups and the right to be forgotten in the GDPR: An uneasy relationship, Computer Law & Security Review: The International Journal of Technology Law and Practice (2018), https://doi.org/10.1016/j.clsr.2018.08.006

Table 2 – Archived objects related to a subscriber.

Name	Payment dates
Surname	Payment amounts
Sex	Payment methods
Address	Amounts owed
Telephone Numbers he has used/using	TIN/TRN
Disconnection dates	Disconnection Reasons
Equipment issued to customer (Routers, SetTopBox, etc.)	Serial Numbers of Equipment Leased or Sold
Service subscription history (e.g. Internet, Cloud Services, etc.)	Messages Issued from company to subscriber
Materials Bought	ID number
Call History (Company to Subscriber and vice versa)	Passport Number

- All previous dunning categories the particular customer has been in.
- Possible disconnections from the Subscription.
- Legal actions taken against the subscriber.

Finally, for every subscriber, regardless of whether she is active or inactive, the data depicted in Table 2 are archived.

Taking the above use cases into consideration one may reasonably deduce that the referenced personal and financial data are necessary for delivering telecommunication services while complying with tax and financial laws, and therefore their retention is not only justified but also mandatory. Any request under the RtbF for removing such data it will most probably collide with tax and financial legislations that oblige their collection, storing, and hence archiving, for a maximum retention period defined under domestic laws. Nevertheless, when this retention period expires businesses are now required to remove these data, from either the production or the backup environment, upon an individual's request for erasure under the RtbF. Notwithstanding this obligation, keeping financial data beyond the predetermined retention period for use in advanced data analytics and automated business decisions provides undeniably a valuable resource for supporting businesses' underlying operations. As a result, new challenges arise for corporations that have to find technical alternatives of exploiting their valuable data stores while not compromising customer's data protection rights such as the RtbF.

6. Conclusions

Legislators deliberately avoided the idea of recommending specific technical frameworks or privacy preserved methods for implementing the legal requirements introduced by the GDPR. Instead, they followed a technology-agnostic approach by specifying the functional requirements in a highly abstracted level, as far as their underlying implementation is concerned, and as such they did not bind the provisions of the law with current trends and state-of-the-art technologies in computer science. The ultimate purpose of this approach was to allow the GDPR's adjustment to future technical innovations. Yet the GDPR's enforcement across the EU mandates businesses and organizations to have operational ready implementations of its requirements in a transparent and efficient manner.

Beyond other challenges that organizations have to face, erasure requests from backups and archives have also become a thorny issue. As our analysis demonstrates, tampering with backups, regardless of whether it is intended or not, is neither a trivial task nor a straightforward process and it is heavily impacted by the data retention regulations and the mediums used for backups. Hence, applying the RtbF requirements on organizations' long-term archival storage it may not only severely affect business operations on tracking and discovering personal information within backed up and archived data, but it will also impose major challenges on advanced ERP data analytics and automated business decisions. Above all, there will be profound implications both for the backup standards, which need to be inevitably aligned with the GDPR provisions, and the search and indexing services, which should expand the current technological limits of data processing.

Acknowledgment

This work was supported by the European Commission under the Horizon 2020 Programme (H2020), as part of the OPERANDO project (Grant Agreement no. 653704).

REFERENCES

American National Standards Institute - ANSI, https://www.ansi.org/. (Accessed 1 September 2018).

Bannon LJ. Forgetting as a feature, not a bug: the duality of memory and implications for ubiquitous computing. CoDesign 2006;2(01):3–15.

Bartolini C, Siry L. The right to be forgotten in the light of the consent of the data subject. Comput Law Secur Rev 2016;32(2):218–37.

Bartolini C, Gheorghe G, Giurgiu A, Sabetzadeh M, Sannier N. Assessing IT security standards against the upcoming GDPR for cloud systems. Proceedings of the Grande region security and reliability day (GRSRD); 2015. p. 40–2.

Blanchette J-F, Johnson DG. Data retention and the panoptic society: the social benefits of forgetfulness. Inform Soc 2002;18(1):33–45.

Canadian Standards Association, Model Code for the Protection of Personal Information (CAN/CSA-Q830-96), 1995. http://cmcweb.ca/eic/site/cmc-cmc.nsf/eng/fe00076.html.

Charter of Fundamental Rights of The European Union (2000/C 364/01) Retrievable from: [cited 18.03.18] Available at: http://www.europarl.europa.eu/charter/pdf/text_en.pdf

Cloud Security Alliance, Cloud controls matrix, https://cloudsecurityalliance.org/group/cloud-controls-matrix/. (Accessed 1 September 2018).

Cloud Standards Customer Council (CSCC). Practical guide to cloud service agreements version 2.0, http://www.cloudcouncil.org/deliverables/CSCC-Practical-Guide-to-CloudService-Agreements.pdf; April 2015.

de Andrade NNG. Oblivion: The right to be different from oneself: reproposing the right to be forgotten. The ethics of memory in a digital age. Springer; 2014. p. 65–81.

de Hert P, Papakonstantinou V. The new general data protection regulation: still a sound system for the protection of individuals? Comput Law Secur Rev 2016;32(2):179–94.

Directive 95/46/EC. Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data. Off J Eur Union 1995;L 281:31–50.

Dodge M, Kitchin R. Outlines of a world coming into existence": pervasive computing and the ethics of forgetting. Environ Plan B Plan Des 2007;34(3):431–45.

European Data Protection Supervisor, Opinion 5/2018. Preliminary opinion on privacy by design, Brussels 2018. https://edps.europa.eu/data-protection/our-work/publications/opinions/privacy-design_en. (Accessed 1 September 2018).

European Data Protection Supervisor, "Opinion of the EDPS on the data protection reform package", https://edps.europa.eu/sites/edp/files/publication/12-03-07_edps_reform_package_en.pdf.

Health Information Privacy, http://www.hhs.gov/ocr/privacy; 2015.

International Organization for Standardization (ISO). (2011). Information technology - Security techniques - Guidelines for auditors on information security controls, ISO/IEC TR 27008:2011, https://www.iso.org/standard/45244.html.

IAPP-EY. IAPP-EY annual privacy governance report 2017, https://iapp.org/media/pdf/resource_center/IAPP-EY-GovernanceReport-2017.pdf; 2018.

Information Systems Audit and Control Association (ISACA): COBIT 5: A business framework for the governance and management of enterprise IT, http://www.isaca.org/COBIT/Pages/default.aspx. (Accessed 1 September 2018).

ISO – International Organization for Standardization, ISO 29100. ISO/IEC 29100:2011 – information technology – security techniques – privacy framework, https://www.iso.org/standard/45123.html; 2011.

ISO – International Organization for Standardization. ISO/IEC 27001:2013 – Information technology – Security techniques information security management systems – Requirements. ISO 27001, https://www.iso.org/standard/54534.html; 2013.

ISO – International Organization for Standardization. ISO/IEC 27002:2013 Information technology – Security techniques code of practice for information security controls. ISO 27002, https://www.iso.org/standard/54533.html ; 2013.

ISO – International Organization for Standardization. Information technology – Security techniques – Storage security, https://www.iso.org/iso/catalogue_detail?csnumber=44404; 2015.

ISO – International Organization for Standardization. ISO/IEC 27018:2014 information technology – Security techniques – Code of practice for protection of personally identifiable information (PII) in public clouds acting as PII processors, http://www.iso.org/iso/catalogue_detail.htm?csnumber=61498; Jul 2014.

ISO – International Organization for Standardization. Information technology – Security techniques – Code of practice for information security controls based on ISO/IEC 27002 for cloud services, https://www.iso.org/iso/catalogue_detail?csnumber=43757 ; 2015.

International Organization for Standardization (ISO). (2015). Information technology - Governance of IT for the organization ISO/IEC 38500:2015 https://www.iso.org/standard/62816.html. (Accessed 1 September 2018).

Joint Task and Initiative, Transformation. Security and privacy controls for federal information systems and organizations, 800. NIST Special Publication; 2013. p.8–13.

Kovacs E. Downtime and data loss cost enterprises $1.7 trillion per year: EMC, SecurityWeek, https://www.securityweek.com/downtime-and-data-loss-cost-enterprises-17-trillion-year-emc. December 2, 2014 (Accessed 1 September 2018).

Kulk S, Borgesius FZ. Google Spain v. González: did the court forget about freedom of expression. Eur J Risk Reg 2014;5:389.

Lyons, D., Weiss, E., Cisler, P., McInerney, P., &Hornkvist, J. (2016). Searching and restoring of backups, U.S. Patent No. 9454587. Washington, DC:U.S. Patent and Trademark Office.

Mantelero A. The EU proposal for a general data protection regulation and the roots of the "right to be forgotten". Comput Law Secur Rev 2013;29(3):229–35.

Mayer-Shönberger V. Delete: The virtue of forgetting in the digital age. Princeton University Press; 2011.

Nene, A.A., Velupula, S.P., Kumar, M., Dhumale, A.V., & Das, A.G. (2011). Backup search agents for use with desktop search tools, U.S. Patent No. 7890527. Washington, DC: U.S. Patent and Trademark Office.

PCI Security Standards Council, Download data security and credit card security standards, https://www.pcisecuritystandards.org/security_standards/.

Pocs M. Will the European Commission be able to standardise legal technology design without a legal method? Comput Law Secur Rev 2012;28:641–50.

Politou E, Alepis E, Patsakis C. Forgetting personal data and revoking consent under the GDPR: challenges and proposed solutions. J Cybersecur 2018.

Regulation (EU) 2016/679. of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation). Off J Eur Union 2016;L 119:1–88.

SAP Access Control, https://www.sap.com/products/access-control.html. (Accessed 1 September 2018).

SAP Data Services, https://www.sap.com/products/data-services.html. (Accessed 1 September 2018).

SAP Information Lifecycle Management, https://www.sap.com/products/information-lifecycle-management.html. (Accessed 1 September 2018).

SAP Information Steward, https://www.sap.com/products/dataprofiling-steward.html. (Accessed 1 September 2018).

SAP Process Control, Charter of Fundamental Rights of The European Union, https://www.sap.com/products/internalcontrol.html. (Accessed 1 September 2018).

Standards Australia, Personal privacy practices for the electronic tolling industry; AS 4721-2000, https://www.standards.org.au/standardscatalogue/sa-snz/. (Accessed 1 September 2018).

Tirosh N. Reconsidering the "Right to Be Forgotten" – Memory rights and the right to memory in the new media era, Media, Culture & Society 39.

Tsaur, Y.P.A., Stringham, R., & Sethumadhavan, S. (2015). Method and apparatus for performing file-level restoration from a block-based backup file stored on a sequential storage device, U.S. Patent No. 9128940. Washington, DC: U.S. Patent and Trademark Office.

Voss WG, Castets-Renard C. Proposal for an international taxonomy on the various forms of the "Right to Be Forgotten": a study on the convergence of norms. Colo Technol Law J 2016;14(2):281–344.